(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 December 2004 (23.12.2004)

PCT

(10) International Publication Number
WO 2004/112310 A1

(51) International Patent Classification[7]: H04L 9/08, 9/32

(21) International Application Number:
PCT/JP2004/008653

(22) International Filing Date: 14 June 2004 (14.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2003-167374 12 June 2003 (12.06.2003) JP

(71) Applicant *(for all designated States except US)*: MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD. [JP/JP]; 1006, Oazakadoma, Kadoma-shi, Osaka 5718501 (JP).

(71) Applicant *(for US only)*: YAMAMICHI, Masami (heir of the deceased inventor).

(72) Inventor: YAMAMICHI, Masato (deceased).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: FUTA, Yuichi. OHMORI, Motoji. TATEBAYASHI, Makoto.

(74) Agent: NAKAJIMA, Shiro; 6F, Yodogawa 5-Bankan, 2-1, Toyosaki 3-chome, Kita-ku, Osaka-shi Osaka 5310072 (JP).

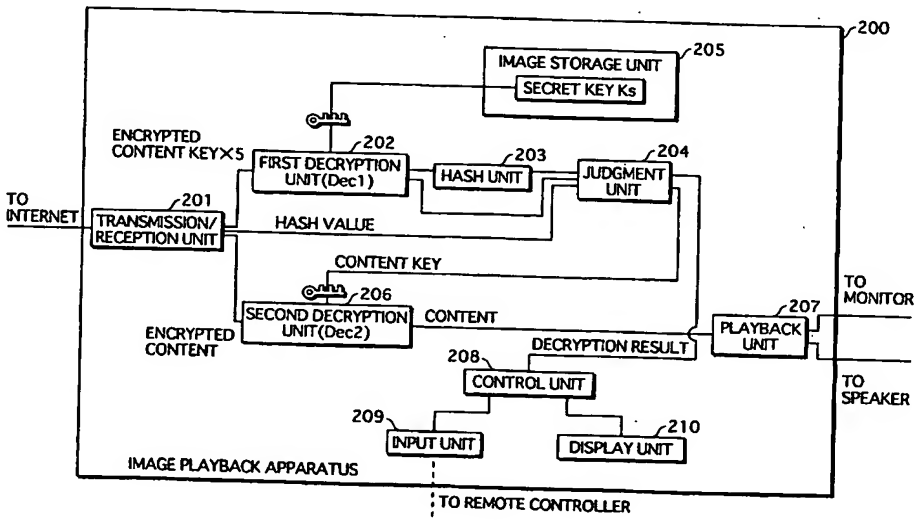
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: ENCRYPTION COMMUNICATION SYSTEM



(57) Abstract: An encroption transmission apparatus and an encryption reception apparatus avoid attack that takes advantage of re-transmission request. A server apparatus encrypts a content key five times, thereby generating five encrypted content keys, calculates a hash value of the content key, and transmits the five encrypted content keys and the hash value. An image playback apparatus receives the five encrypted content keys and the has value, decrypts the five encrypted content keys thereby generating five content keys, calculates hash values each corresponding to the generated content keys, and compares the calculated hash values with the received hash value respectively. If at least one of the five calculated hash values matches the received hash value, the corresponding content key is considered correct. Conversely, if none of the five calculated hash values matches the received hash value, it is considered a decryption error.

WO 2004/112310 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.